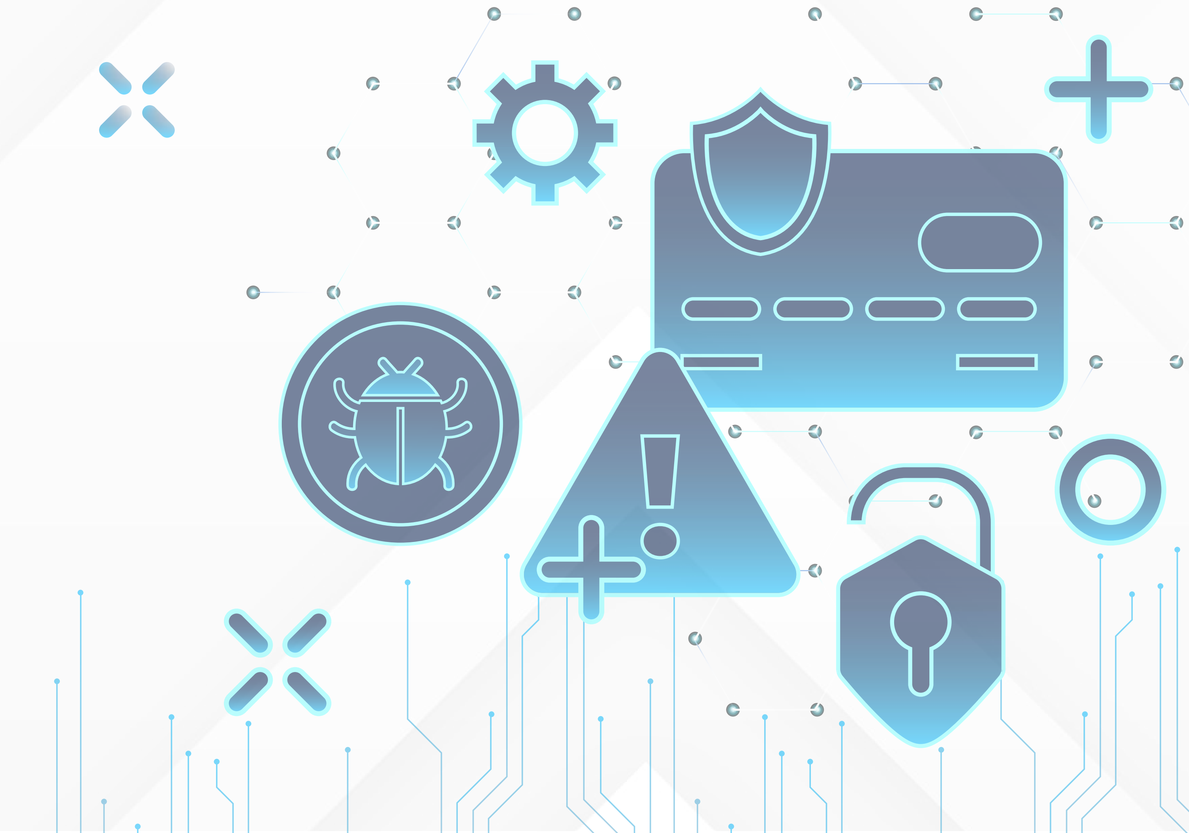
كتيب

استخدام اطار MITRE ATT&CK في الكشف عن الهجمات المتقدمة

بالتعاون مع:
د. عادل الشمراني



المحتويات

منشآت
monsha'at
هيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

عن مركز ذكاء

جاء إنشاء مركز ذكاء كأول مركز متخصص في التقنيات المتقدمة لخدمة رواد الأعمال والمنشآت الصغيرة والمتوسطة في المملكة. يهدف المركز لتمكين قطاع المنشآت الصغيرة والمتوسطة من توظيف التقنيات المتقدمة لتطوير هذه المنشآت وزيادة تنافسيتها وأن يكون حلقة ربط ما بين رواد الأعمال وصناع القرار في مجالاته المتخصصة.

يتخذ مركز ذكاء لعلوم البيانات والذكاء الاصطناعي مدينة الخبر مقرًا له، ويقع مركز ذكاء لإنترنت الأشياء والأمن السيبراني في مدينة الرياض، ويخدم المركز بفرعَيه شتى أنحاء المملكة العربية السعودية.

بإمكانك النقر على الشعارات والروابط الموجودة في هذا الكتيب للذهاب إلى المواقع الإلكترونية الخاصة بها.

سياسة الاستخدام

إن المعلومات الواردة في هذا الكتيب تم تجميعها وتنسيقها بجهود موظفي مركز ذكاء التابع لـ الهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت"، ولا ينبغي لقارئها أن يعمل بها دون مشورة مناسبة من المتخصصين.

للمزيد من المعلومات نرجو التواصل على البريد الإلكتروني support@thakaa.sa

عن الكتيب:

تم جمع وبناء محتوى هذا الكتيب كملخص لاستخدام اطار MITRE ATT&CK للحد من الهجمات السيبرانية، وتم الاستناد في هذا الكتيب على معلومات تم جمعها من الموقع الرئيسي لمؤسسة MITRE، وأيضا من خلال خبرة عملية في استخدام هذا الإطار وخاصة فيما يتعلق بأنشطة ال Red Team.

ماذا يقدم؟

يقدم هذا الكتيب وصف لإطار MITRE ATT&CK وآلية استخدامه للكشف عن مراحل الهجمات السيبرانية وتصنيفها وربطها بالأحداث التي يتم اكتشافها من خلال حلول الأمن السيبراني. ويساعد هذا الاكتشاف إلى التبكير في تعطيل مراحل الهجوم السيبراني قبل أن يتسبب بآثار سلبية على الضحية.

ماهو إطار MITRE ATT&CK:

- إطار MITRE ATT&CK هو نموذج شامل لفهم وتصنيف تقنيات الهجمات الإلكترونية.

- يُعد ATT&CK اختصارًا لـ "Adversarial Tactics, Techniques, and Common Knowledge"، وتم تطويره بواسطة مؤسسة MITRE وهي منشأة أمريكية غير هادفة للربح، تأسست سنة 1958 من معهد ماساتشوستس للتكنولوجيا MIT. تعمل MITRE في مجال البحث والتطوير التي تخدم القطاعات الحكومية الأمريكية في مجالات مختلفة، مثل الدفاع والطيران، والرعاية الصحية، والامن السيبراني.

- ويهدف هذا الإطار إلى توفير لغة مشتركة وشاملة لفهم مراحل الهجمات السيبرانية التي يستخدمها الخصم.

- يتألف إطار MITRE ATT&CK من قائمة شاملة من التكتيكات Tactics والتقنيات التي يمكن استخدامها في الهجمات السيبرانية.

- ينقسم الإطار إلى عدة مجموعات رئيسية تشمل على تقسيمات فرعي، تم تصنيفها بهيكلية مستقاه من مراحل هجوم سيبرانية مستقاه من حوادث سيبرانية حقيقية. تشتمل المجموعات الرئيسية للإطار على تكتيكات وتقنيات، أما التقسيمات الفرعية فهي مخصصة أكثر، تهدف لمساعدة محللي الهجمات السيبرانية على موائمة ما يتم رصده من هجمات بمراحل الهجوم المعرفة في الإطار.

- يعمل إطار MITRE ATT&CK كأداة قوية لفهم وتصنيف الهجمات الإلكترونية. يمكن استخدامه لتحليل وتصنيف الهجمات السابقة وتحديد الأنماط والأنشطة الضارة وتحديد الثغرات الأمنية في البنية التحتية الرقمية لمنظمة ما.

- يوفر ATT&CK إطارًا لتطوير استراتيجيات الدفاع واستراتيجيات الرصد والاستجابة للحماية من هجمات مماثلة في المستقبل.

- باختصار، إطار MITRE ATT&CK هو أداة هامة لفهم وتصنيف الهجمات الإلكترونية وتعزيز قدرة المؤسسات على حماية بيئتها الرقمية من الهجمات الضارة.

المعلومات المتوفرة التي يمكن الاستفادة منها من خلال الإطار:

إطار MITRE ATT&CK يحتوي على مجموعة كبيرة من المعلومات المتعلقة بتكتيكات وتقنيات الهجمات الإلكترونية. هذه المعلومات تشمل التكتيكات المستخدمة من قبل المهاجمين والأنشطة والتقنيات المرتبطة بها. وفيما يلي نظرة عامة عن المعلومات المشمولة في إطار MITRE ATT&CK:

التكتيكات (Tactics):

والتي تعتبر السبب الذي يجعل الخصم يقدم على خطوة معينة لتحقيق هدف في مدة قصيرة، بحيث يساعد على الانتقال لمرحلة أكثر تقدماً ضمن سلسلة مراحل الهجوم. يوجد في الإطار عدة تكتيكات تستخدمها المجموعات المهاجمة لتحقيق أهدافها. تشمل بعض التكتيكات التعرف على المستهدفين، والاستيلاء على الحسابات، وتنفيذ البرمجيات الخبيثة، والتحرك داخل الشبكة، والحفاظ على الوصول.

التقنيات (Techniques):

والتي تعتبر الوسيلة والأدوات المستخدمة لتنفيذ الهجمات في عدة مراحل. ويحتوي الإطار على مجموعة واسعة من التقنيات التي يستخدمها المهاجمون لتنفيذ التكتيكات السابقة. على سبيل المثال، قد تشمل التقنيات استخدام البرمجيات الخبيثة مثل الفيروسات وبرامج التجسس وحصان طروادة، واستغلال الثغرات في البرمجيات، واستخدام هجمات القرصنة المتقدمة مثل الهجمات الموجهة والتصيّد الهندسي.

المجموعات (Groups):

يُعرف في الإطار مجموعات هجمات معينة معروفة تقوم بتنفيذ التقنيات المذكورة سابقًا. يتم تصنيف هذه المجموعات بناءً على الأنشطة والأهداف المشتركة لها. وتعمل هذه المجموعات كنماذج تصورية للمهاجمين وتساعد في تحليل الهجمات السابقة وتعرف النماذج القائمة.

المصادر والمراجع (References):

يتضمن الإطار مجموعة من المصادر والمراجع التي يمكن الاستناد إليها للحصول على مزيد من التفاصيل والمعلومات حول كل تكتيك وتقنية ومجموعة.

المعلومات المتوفرة التي يمكن الاستفادة منها من خلال الإطار:

هنا سوف نقوم بذكر بعض الأمثلة لكلاً من المكونات الأساسية:

التكتيكات (Tactics):

التعرف على المستهدفين (مرحلة الاستطلاع) (Reconnaissance):

يتعلق بجمع المعلومات المتاحة عن الضحايا المحتملين، مثل البحث عن عناوين البريد الإلكتروني والتجسس على الشبكات الاجتماعية.

تطوير الموارد (Resource Development):

يتضمن تكتيك تطوير الموارد قيام المهاجم بإنشاء أو شراء أو سرقة الموارد التي يمكن استخدامها لدعم عمليات الهجوم على الضحية. تتضمن هذه الموارد البنية التحتية أو الحسابات في الأنظمة المختلفة لدى الضحية. يمكن للمهاجم الاستفادة من هذه الموارد للمساعدة في المراحل الأخرى من الهجمة، مثل استخدام حسابات البريد الإلكتروني للتصيد الاحتيالي كجزء من الوصول المبدئي.

الوصول بشكل أولي (Initial Access):

يتعلق بإدخال البرمجيات الخبيثة إلى البنية التحتية المستهدفة، سواءً كان ذلك عن طريق البريد الإلكتروني المصاب أو الثغرات في البرمجيات.

التحرك داخل الشبكة (Lateral Movement):

يتعلق بتحرك المهاجم داخل البنية التحتية بعد الاستيلاء الأولي، واختراق أجهزة أخرى والتحكم بها.

الحفاظ على الوصول (Persistence):

يتعلق بالإجراءات التي يتخذها المهاجم للحفاظ على وصوله إلى البنية التحتية المستهدفة والتخفي وعدم الكشف عنه.

المعلومات المتوفرة التي يمكن الاستفادة منها من خلال الإطار:

هنا سوف نقوم بذكر بعض الأمثلة لكلاً من المكونات الأساسية:

التقنيات (Techniques):

استخدام البرمجيات الخبيثة (Malware):

يتضمن استخدام برامج خبيثة مثل الفيروسات وبرامج التجسس وحصان طروادة للتسلل والتلاعب بالأنظمة والبيانات.

استغلال الثغرات (Exploits):

يشير إلى استغلال الثغرات الموجودة في البرمجيات أو الأجهزة للوصول غير المصرح به أو تنفيذ أوامر ضارة.

التصيّد الهندسي (Social Engineering):

يتعلق باستخدام الخداع والتأثير النفسي على الأفراد للحصول على معلومات حساسة أو الوصول إلى الأنظمة.

الحركة الجانبية (Lateral Movement):

يشير إلى قدرة المهاجم على الانتقال من جهاز إلى آخر داخل الشبكة المستهدفة، واستغلال الاختلالات والضعف في الأمان للتحرك بحرية.

التشويش (Evasion):

يشمل استخدام تقنيات للتخفي وتجنب اكتشاف الهجمات، مثل تشفير الاتصالات أو تعديل البرامج الضارة لتجنب التوقعات الأمنية.

المعلومات المتوفرة التي يمكن الاستفادة منها من خلال الإطار:

الأمثلة:

هنا سوف نقوم بذكر بعض الأمثلة لكلاً من المكونات الأساسية:

المجموعات (Groups):

يعرف في الإطار عدد من المجموعات الهجومية المعروفة التي تستخدم تقنيات معينة. على سبيل المثال، APT29 وAPT32 وFIN7 وغيرها من المجموعات المعروفة والتي يتم تصنيفها بناءً على نشاطها ونمط هجماتها.

المصادر والمراجع (References):

يحتوي الإطار على قائمة مصادر ومراجع يمكن الاستناد إليها للحصول على مزيد من المعلومات حول كل تكتيك وتقنية ومجموعة، بما في ذلك مستندات MITRE وتقارير الهجمات السابقة والأبحاث المعترف بها.

هذه المعلومات في إطار MITRE ATT&CK تساعد المؤسسات على فهم الأنشطة الهجومية المحتملة وتوجيه جهودها لتحليل الهجمات السابقة وتصميم استراتيجيات الدفاع والاستجابة الفعالة لحماية الأنظمة والبيانات الحساسة.

طرق دمج الإطار مع المؤسسات تقنياً:

الأمثلة:

هناك عدة طرق يمكن استخدامها لدمج إطار MITRE ATT&CK مع المؤسسات تقنيا. إليك بعض الطرق الشائعة:

تقييم الثغرات:

يمكن استخدام إطار MITRE ATT&CK لتقييم الثغرات والضعف في البنية التحتية الرقمية للمؤسسة. يتم تحليل التكتيكات والتقنيات المستخدمة في ATT&CK لتحديد الثغرات التي يمكن استغلالها وتعزيز الأمان.

تصميم استراتيجيات الدفاع:

باستخدام إطار MITRE ATT&CK، يمكن تطوير استراتيجيات الدفاع الموجهة لمكافحة التهديدات الأمنية. يمكن استنتاج أفضل الممارسات وتوجيهات الأمان من التكتيكات والتقنيات المشمولة في ATT&CK لتصميم نماذج الدفاع الفعالة.

رصد واستجابة الهجمات:

يمكن استخدام إطار MITRE ATT&CK لتحسين قدرة المؤسسة على رصد الهجمات والاستجابة لها. من خلال عمل مواءمة لأنشطة الهجمات الحالية مع التكتيكات والتقنيات الموجودة في ATT&CK، يمكن تحديد نمط الهجمات واتخاذ إجراءات استجابة فورية ومناسبة.

تدريب الفرق الأمنية:

يمكن استخدام إطار MITRE ATT&CK كأداة تدريبية لتعزيز مهارات فرق الأمن الداخلية. يمكن توظيف ATT&CK في تنظيم تدريبات ومحاكاة سيناريوهات هجومية وتطوير قدرات الكشف والتحليل والاستجابة.

تكامل أدوات الأمان:

يمكن تكامل إطار MITRE ATT&CK مع أدوات الأمان المستخدمة في المؤسسة، مثل أنظمة الكشف عن التهديدات وإدارة الحوادث والأنظمة الأمنية الأخرى. يمكن استخدام ATT&CK كنموذج لتحسين قدرة هذه الأدوات على تحليل وتصنيف الأنشطة الضارة وتنفيذ الاستجابة المناسبة.

يجب ملاحظة أن دمج إطار MITRE ATT&CK يتطلب تخطيطًا وتنفيذًا مناسبًا وتعاونًا بين فرق الأمن والشبكات والأنظمة في المؤسسة. قد يتطلب ذلك التدريب والتوعية والتنسيق لضمان استخدام الإطار بشكل فعال ومناسب لاحتياجات المؤسسة.

دمج إطار MITRE ATT&CK مع مركز العمليات الأمنية Security Operation Center (SOC)

مركز العمليات الأمنية (SOC) هو وحدة أو فريق متخصص داخل مؤسسة يتولى مهمة مراقبة واستجابة الأمان. يهدف SOC إلى رصد وتحليل واكتشاف الأنشطة الاستباقية والهجمات السيبرانية المستهدفة للمؤسسة، واتخاذ الإجراءات اللازمة للتصدي لهذه الهجمات وحماية الأصول والبيانات الحساسة.

تعتمد وظائف SOC على الكشف المستمر والتحليل والاستجابة الفورية للتهديدات الأمنية. يعتمد SOC على تقنيات متقدمة مثل تحليل السلوك، ورصد الأنماط الاستباقية، واستخدام أدوات الكشف والتحليل وإدارة الحوادث الأمنية.

دور SOC يشمل:

رصد الأنشطة:

يتم رصد الشبكات والأنظمة والأجهزة المستخدمة في المؤسسة للكشف عن أي نشاط مشبوه أو غير مصرح به.

التحليل والتحقق:

يتم تحليل الأحداث والبيانات المتعلقة بالأنشطة المشتبه فيها لتقييم مدى تهديدها ومدى التأثير المحتمل.

الاستجابة والتعزيز:

يتم اتخاذ إجراءات للتصدي للهجمات المكتشفة وإزالتها من النظام. يتم أيضًا تعزيز الأمان وتحسين الإجراءات والتدابير للوقاية من هجمات مستقبلية.

يعد SOC جزءًا حاسمًا في استراتيجية الأمان لأي مؤسسة، حيث يساعد في تعزيز الاستجابة السريعة للتهديدات الأمنية وحماية الأصول والبيانات الحساسة.

الاستفادة من إطار MI TRE ATT&CK في مركز العمليات الأمنية Security Operation Center (SOC)

عملية دمج إطار MITRE ATT&CK مع مركز العمليات الأمنية (SOC) تعتمد على عدة عناصر وممارسات. إليك بعض الخطوات التي يمكن اتخاذها لدمج الإطار مع SOC :

تدريب فرق SOC: يجب توفير التدريب والتوعية لفرق SOC بشأن إطار MI-TRE ATT&CK ومفاهيمه واستخداماته. ينبغي على أعضاء فرق SOC فهم التصنيفات والتكتيكات والتقنيات المشمولة في ATT&CK وكيفية تطبيقها في عمليات الكشف والاستجابة.

إنشاء مصادر معلومات ATT&CK: ينبغي تجهيز فرق SOC بمصادر معلومات موثوقة حول إطار MITRE ATT&CK وتحديثاته المستمرة. يمكن الاستناد إلى موقع MITRE ATT&CK الرسمي والمنشورات والوثائق ذات الصلة للحصول على معلومات حديثة حول التهديدات والتقنيات الجديدة.

توفير أدوات الكشف والتحليل: يمكن تكامل أدوات الكشف والتحليل المستخدمة في SOC مع إطار MITRE ATT&CK. يتيح ذلك لفرق SOC ربط الأنشطة والأحداث المشتبه فيها بالتصنيفات والتكتيكات والتقنيات المعرفة في ATT&CK، وبالتالي تعزيز قدرتهم على اكتشاف واستجابة الهجمات.

الاستفادة من إطار MI TRE ATT&CK في مركز العمليات الأمنية Security Operation Center (SOC)

تطبيق قواعد الكشف: يجب تطوير قواعد الكشف المبنية على إطار MITRE ATT&CK. يمكن لفرق SOC تصميم قواعد الكشف التي تستند إلى النشاط الضار المعروف والسلوك المرتبط بالتصنيفات والتكتيكات والتقنيات في ATT&CK. يتم استخدام هذه القواعد للكشف عن الأنشطة الاستباقية والهجمات المحتملة.

التحليل والتقارير: يمكن لفرق SOC تحليل الأحداث والتقارير المتعلقة بالتصنيفات والتكتيكات والتقنيات في إطار ATT&CK. يساعد هذا التحليل في فهم أنماط الهجمات وتوجيه استجابة SOC بشكل فعال واتخاذ الإجراءات اللازمة لحماية المؤسسة.

بشكل عام، تتطلب عملية دمج إطار MITRE ATT&CK مع SOC التركيز على التدريب والتوعية وتكامل الأدوات وتصميم قواعد الكشف وتحليل الأحداث. هذا يساعد في تحسين قدرة SOC على الكشف عن الهجمات والتصدي لها بشكل فعال. هذا مجرد مثال توضيحي، وقد يختلف التطبيق الفعلي من مؤسسة لأخرى وفقًا لاحتياجاتها ومتطلباتها الخاصة.

استفادة فريق Red Team من إطار MITRE ATT&CK

فريق Red Team يمكنه الاستفادة من إطار MITRE ATT&CK في عدة طرق ومنها:

- تحليل الهجمات: يمكن لفريق Red Team استخدام إطار MITRE ATT&CK كأداة لتحليل الهجمات وتقييم فعالية أدوات وتقنيات الهجوم. يمكنهم تصنيف أنشطتهم واستخدامها لفحص الأمان الشامل للنظام وتحديد الثغرات ونقاط الضعف المحتملة.

- إرشاد الاختبارات: يمكن لفريق Red Team استخدام ATT&CK كمرجع لتوجيه عمليات اختبار الاختراق. يمكنهم تصميم السيناريوهات الهجومية وفقًا للتصنيفات والتكتيكات والتقنيات الموجودة في ATT&CK لتحاكي تقنيات الهجوم الحديثة والهجمات المستهدفة.

- تطوير تقارير الاختبار: يمكن لفريق Red Team استخدام ATT&CK لتوضيح نتائج اختبارات الاختراق وتقديم تقارير شاملة لفرق الدفاع. يمكنهم استخدام التصنيفات والتكتيكات والتقنيات في ATT&CK لوصف الأنشطة الهجومية والتأثيرات المحتملة على المؤسسة.

- تعزيز الوعي الأمني: يمكن لفريق Red Team استخدام ATT&CK كأداة لتعزيز الوعي الأمني في المؤسسة. يمكنهم تقديم تقارير وتوضيحات حول التهديدات والتقنيات المستخدمة في الهجمات وتوجيه الإجراءات الوقائية والتدابير الأمنية اللازمة لتعزيز الدفاع.

من خلال استخدام إطار MITRE ATT&CK، يمكن لفريق Red Team تحسين قدراتهم وتوجيه جهودهم لتنفيذ هجمات مستهدفة وتقييم فعالية الأدوات والتقنيات المستخدمة في الدفاع عن المؤسسة.

استفادة فريق Red Team من إطار MITRE ATT&CK

مثال:

وفيما يلي تفاصيل إضافية حول كيفية استفادة فريق (Red Team) من إطار MITRE ATT&CK في تحليل الهجمات:

تحليل الهجمات:

- يتم استخدم إطار MITRE ATT&CK كأداة قوية لتحليل الهجمات وفهم النشاط الهجومي المستهدف للمؤسسة. يمكن للفريق استخدام التصنيفات الرئيسية في ATT&CK لتصنيف الأنشطة الهجومية وتحليلها بناءً على تكتيكات الهجوم المستخدمة.

تصنيف الأنشطة الهجومية:

- يتم استخدم تصنيفات ATT&CK لتصنيف الأنشطة الهجومية المكتشفة أثناء عمليات الاختراق. يمكنهم استخدام التصنيفات الموجودة في ATT&CK لتحديد ما إذا كانت الأنشطة الهجومية تندرج تحت تصنيف الاستطلاع (Reconnaissance) أو الحصول على امتيازات (Privilege Escalation) أو غيرها من التصنيفات.

تحليل التكتيكات والتقنيات:

- يستخدم فريق تكتيكات وتقنيات ATT&CK لفهم كيفية تنفيذ الهجمات واستخدام التقنيات الخاصة بالمهاجمين. يتحقق الفريق من التكتيكات والتقنيات المستخدمة في ATT&CK ويقوم بتحليلها لتحديد أدوات الهجوم والأنماط المعتادة والسلوك الهجومي النموذجي.

توثيق الأنشطة الهجومية:

- يقوم الفريق بتوثيق الأنشطة الهجومية وفقًا للتصنيفات والتكتيكات والتقنيات في ATT&CK. يسجلون المعلومات المتعلقة بالأنشطة الهجومية والأدوات المستخدمة والتحركات المستهدفة والأنظمة المستهدفة. تساعد هذه الوثائق في توثيق أدلة الهجوم وتحليلها فيما بعد.

تحليل نقاط الضعف:

- يتمكن الفريق من استخدام التصنيفات والتكتيكات والتقنيات في ATT&CK لتحليل نقاط الضعف في الدفاع الأمني للمؤسسة. من خلال مقارنة النشاط الهجومي المكتشف بنماذج الهجمات الموجودة في ATT&CK، يمكنهم تحديد الثغرات والنقاط الضعيفة والمساعدة في تحسين الدفاع واتخاذ التدابير اللازمة لحماية المؤسسة.

تستخدم هذه العمليات التحليلية المختلفة في استخلاص معلومات قيمة حول النشاط الهجومي وتقديم تقارير شاملة للمؤسسة، مما يساعد فرق الدفاع على فهم تهديدات الأمان وتعزيز استعدادهم لمواجهة هذه التهديدات.

استفادة فريق Red Team من إطار MITRE ATT&CK

مثال:

هناك العديد من الأدوات التي يمكن استخدامها من قبل فريقRed Team ويمكن ربطها بإطار MITRE ATT&CK لتسهيل عمليات التحليل والاختبار وهنا بعض الأمثلة على هذه الأدوات:

Cobalt Strike

- تعتبر Cobalt Strike أداة شهيرة في مجال اختبار الاختراق وتستخدم بشكل واسع من قبل فرق الهجوم الأحمر. يمكن استخدامها لتنفيذ هجمات اختبار الاختراق ومحاكاة سلوك المهاجمين وتحليل النتائج وتقديم التقارير. يمكن ربط استخدام Cobalt Strike بإطار MITRE ATT&CK من خلال توثيق الأنشطة الهجومية وتحديد التصنيفات والتكتيكات والتقنيات المستخدمة.

Metasploit Framework

- يعد Metasploit Framework واحدًا من أشهر أدوات اختبار الاختراق المتاحة. يوفر مجموعة واسعة من الاستغلالات والأدوات لتنفيذ هجمات اختبار الاختراق. يمكن ربط استخدام Metasploit Framework بإطار MITRE ATT&CK من خلال تحليل الأنشطة الهجومية والتصنيفات والتكتيكات والتقنيات المستخدمة.

Empire

- تعتبر Empire أداة متعددة المنصات تستخدم لاختبار الاختراق ومحاكاة الهجمات. توفر مجموعة من الوحدات والأدوات لتنفيذ هجمات متنوعة. يمكن ربط استخدام Empire بإطار MITRE ATT&CK من خلال توثيق الأنشطة الهجومية وتحليلها ومطابقتها مع التصنيفات والتكتيكات والتقنيات.

Atomic Red Team

- تعتبر Atomic Red Team مجموعة من السيناريوهات والأدوات المصممة لمحاكاة تقنيات الهجوم المعروفة. يمكن استخدام Atomic Red Team لتنفيذ اختبارات الاختراق واختبار فعالية الدفاع الأمني للمؤسسة. يمكن ربط استخدام Atomic Red Team بإطار MITRE ATT&CK عن طريق مطابقة السيناريوهات والتقنيات المستخدمة في ATT&CK مع نتائج الاختبار.

هذه مجرد بعض الأمثلة على الأدوات المستخدمة في فرق الهجوم الأحمر والتي يمكن ربطها بإطار MITRE ATT&CK. هناك المزيد من الأدوات المتاحة ويمكن اختيار الأدوات المناسبة حسب احتياجات الفريق ومتطلبات الاختبار.

حدود المسؤولية

تقدم منشآت المصادر التعليمية وهي خدمة من خدمات مكتبة مركز ذكاء التي تقدمها منشآت والتي تساهم وتساعد في إثراء المحتوى العربي لمصادر التعلم عبر الإنترنت لتوفير المعرفة لفئات مختلفة في مجالات التقنية وريادة الأعمال، ولا تقدم "منشآت" أو من يمثلها أيّ قرارات أو ضمانات سواءً بشكل صريح أو ضمني حول اكتمال أو دقة أو موثوقية أو ملاءمة أو توافر هذه البيانات أو المعلومات أو المواد ذات الصلة الواردة في الكتيّب لأي غرض كان ولا يجوز استخدامها لغرض آخر غير الاستخدام العام ولا تتحمل "منشآت" أو من يمثلها – بأي حال من الأحوال- أي أضرار مادية أو معنوية، مباشرة أو غير مباشرة قد تحصل، وتؤكد "منشآت" أو من يمثلها أنها غير مسؤولة سواءً بشكل كامل أو جزئي عن أي ضرر مباشر أو غير مباشر، عرضي أو تبعي أو عقابي خاصًا كان أو عامًا، كما أنها غير مسؤولة عن أي فرصة ضائعة أو خسارة أو ضرر من أي نوع، ومنها على سبيل المثال لا الحصر، أي ضرر أو فيروس قد يتعرض له الحاسوب الشخصي نتيجة الدخول إلى هذه الصفحة، وأن "منشآت" أو من يمثلها تبذل الجهد للتأكد من أن المعلومات المتوفرة من خلال المصادر التعليمية شاملة ودقيقة قدر المستطاع. وكما تؤكد "منشآت" على الالتزام بحقوق النشر وحقوق الملكية الفكرية لمحتويات المصادر التعليمية بما في ذلك شعار "منشآت" ولا يحق نشر أي معلومات أو رأي يتم التعبير عنه هنا دون الحصول على إذن خطي مسبق للقيام بذلك من قبل "منشآت".

منشآت
monsha'at
هيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

ولمعرفة المزيد وإمكانية تطبيق والاستفادة من الاطار من الممكن

حجز استشارة

مع د. عادل الشمراني

شكرًا لكم

Thakaa.sa